DOI: 10.15199/ELE-2014-203

Analiza stanu zastosowań podpisu elektronicznego w Polsce

dr inż. WOJCIECH NOWAKOWSKI, prof. nazw., Instytut Maszyn Matematycznych, Warszawa

Pojęcie „podpis elektroniczny" (*electronic signature*) zostało wprowadzone do prawa gospodarczego przez unijną Dyrektywę 1999/93/UE [1]. Dyrektywa ta określa, że podpis elektroniczny jest operacją podpisywania konkretnych danych (dokumentu elektronicznego) przez osobę fizyczną. Podpis ten jest w istocie dodatkową informacją cyfrową dołączoną do przesyłanego dokumentu elektronicznego służącą do weryfikacji jej źródła.

W ciągu piętnastu już lat obowiązywania pierwszego dokumentu dotyczący wspólnotowych ram podpisu elektronicznego w UE, czyli wspomnianej Dyrektywa 1999/93/UE nie odnotowano oczekiwanego nasycenia rynku podpisów elektronicznych. Dopiero w kwietniu 2014 roku Parlament Europejski przyjął projekt rozporządzenia eIDAS [2] o „identyfikacji elektronicznej i usługach zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym". Rozporządzenie to, oprócz kwalifikowanego podpisu elektronicznego, definiuje także dodatkowe usługi kwalifikowane: znakowanie czasem, usługę e-doręczenia, pieczęć elektroniczną, usługę walidacji oraz usługę uwierzytelnienia witryny internetowej.

W Polsce pojęcie podpisu elektronicznego zdefiniowano w bardzo nieprecyzyjnej ustawie z września 2001 roku [3], uważanej do dziś za bubel prawny. W ustawie tej nie wymuszono stosowania mechanizmów opartych na kryptografii asymetrycznej i funkcjach skrótu. Za podpis elektroniczny zgodny z ustawą można więc np. uznawać podpis składany pod elektroniczną deklaracją PIT kwotą przychodu za poprzedni rok podatkowy. Co więcej, w przepisie art. 8 tej ustawy czytamy: „Nie można odmówić ważności i skuteczności podpisowi elektronicznemu tylko na tej podstawie, że istnieje w postaci elektronicznej lub dane służące do weryfikacji podpisu nie mają kwalifikowanego certyfikatu, lub nie został złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu elektronicznego". Natomiast w tejże ustawie szczegółowo uregulowany jest tylko jeden z rodzajów podpisu, czyli tzw. bezpieczny podpis elektroniczny i to tylko taki, który jest weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu! Bublem prawnym jest również główne rozporządzenie techniczne podpisu elektronicznego w Polsce z 2002 roku [4].

Obecnie całą sferę podpisu elektronicznego oraz jego stosowania obejmuje ponad 30 głównych i uzupełniających aktów prawnych różnej wagi, zupełnie niekompletnych, często sprzecznych ze sobą.

Ciągle trwają prace nad dwoma głównymi projektami prawnymi dotyczącymi podpisu elektronicznego, właśnie wspomnianego Rozporządzenia i Ustawy zmierzające (po 13 latach!) do dostosowania polskiego prawa do wymogów stawianych w dyrektywie 1999/93/EC oraz norm europejskich. Jednocześnie w Unii Europejskiej także trwają prace nad nowelizacją dyrektywy 1999/93/EC o podpisach elektronicznych.

Co więcej, nawet te nowe regulacje prawne nie zlikwidują ograniczeń stosowania podpisu elektronicznego, które bezpośrednio wynikają z immanentnych, technicznych i prawnych cech obecnych procedur. Dotyczy to np. podpisywania dokumentów dotyczących ksiąg wieczystych, które muszą być przechowywane przez 50 lat, a które po 20 latach od podpisania elektronicznego staną się nieweryfikowalne gdyż okres przechowywania certyfikatów klucza publicznego w repozytorium wynosi lat 20. Dotyczy to także np. notariatu, urzędów stanu cywilnego, urzędów patentowych czy sfery urbanistyki i zagospodarowania przestrzennego. W tych ostatnich przypadkach chodzi również o to, że podpisem elektronicznym w obecnej postaci nie da się podpisywać klasycznymi algorytmami form graficznych: rysunków, oznaczeń geograficznych, topografii układów scalonych czy planów zagospodarowanie przestrzennego. Nawet szumnie ogłoszona w 2012 roku procedura zdalnej rejestracji spółek przez internet w oparciu o instrumentarium podpisu elektronicznego jest cząstkowa i nie działa poprawnie [5].

Rys. 1. Karta podpisu elektronicznego w czytniku
Fig. 1. Electronic signature card reader

Nieco teorii i o procedurze podpisu elektronicznego

Podpis elektroniczny opiera się na kryptografii asymetrycznej (klucza publicznego). Znanych jest kilka algorytmów szyfrowania asymetrycznego. Najszerzej stosowanym jest system RSA [6], opracowany w 1977 r. przez Rona Rivesta, Adi Shamira oraz Leonarda Adlemana w MIT. Jest to jednocześnie pierwszy algorytm asymetryczny, który można stosować zarówno do szyfrowania wiadomości jak i do podpisów cyfrowych. Bezpieczeństwo tego algorytmu opiera się na niesymetrii trudności numerycznej dwóch procesów: obliczenia iloczynu liczb pierwszych, co jest niezbędne do generacji pary kluczy oraz faktoryzacji tego iloczynu (wyznaczaniu czynników pierwszych) dużych liczb złożonych, co byłoby niezbędne do złamania tego algorytmu. To drugie może najszybszym komputerom zajmować lata.

Procedury kryptografii asymetrycznej, w przeciwieństwie do procedur symetrycznych są stosunkowo wolne i wymagają dużych mocy obliczeniowych, zwłaszcza do większych dokumentów. Dlatego w podpisie elektronicznym stosuje się tzw. *jednokierunkowe funkcje skrótu* (*hash*). Są to przekształcenia matematyczne zamieniające ciąg bitów dowolnej długości w inny ciąg bitów o zadanej z góry określonej długości, od których oczekuje się, że:

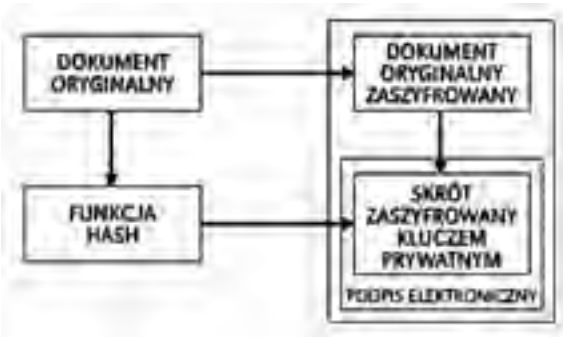
– nie nastąpi wygenerowanie dwóch wiadomości o takim samym skrócie, czyli nie nastąpi tzw. kolizja (realnie, bo z czysto matematycznego punktu widzenia wiadomo, że jeśli funkcja wyj-

ściowa jest 128-bitówowa, to w $2^{128}+1$ wynikach na pewno coś się powtórzy),
– nie jest możliwe odtworzenia danych wejściowych na podstawie skrótu.

Zastosowanie funkcji skrótu umożliwia następującą, przyspieszoną procedurę podpisu elektronicznego: nadawca najpierw tworzy skrót a następnie podpisuje ten skrót szyfrując go kluczem prywatnym i przesyła wraz z dokumentem odbiorcy. Odbiorca używa tej samej funkcji haszującej do otrzymania skrótu dokumentu, a następnie deszyfruje podpisany skrót używając klucza publicznego nadawcy. Jeżeli zdeszyfrowany skrót zgadza się z przesłanym, to podpis jest prawdziwy. Zalety tej procedury są oczywiste: podpis jest znacznie krótszy od dokumentu, a jego wiarygodność można sprawdzić bez oglądania samego dokumentu. W praktyce sam przesyłany dokument jest również szyfrowany, ale już jakimkolwiek szybkim algorytmem symetrycznym, np. DES.

Praktyczna procedura złożenia podpisu pod przygotowanym wcześniej dokumentem elektronicznym jest następująca. W pierwszym kroku obliczany jest skrót dokumentu. Jest on przesyłany do karty kryptograficznej. Tam wykonywane jest szyfrowanie tego skrótu, np. według algorytmu RSA za pomocą klucza prywatnego zapisanego na tej karcie. Warunkiem wykonania tej operacji jest jej uwierzytelnienie kodem PIN. Wygenerowane dane odsyłane są do komputera i dołączane do oryginalnego dokumentu. Dodatkowo do dokumentu oraz zaszyfrowanego skrótu dołączany zostaje certyfikat zawierający dane osoby składającej podpis oraz jej klucz publiczny. Tak przygotowane dane można nazwać podpisem elektronicznym dokumentu i z nim powiązanym (*rys. 2*).

Zastosowanie technik kryptograficznych w procedurze podpisu elektronicznego nie wystarcza aby być pewnym, że przesłany dokument jest właściwy. Zaszyfrowanie lub elektroniczne podpisanie dokumentu nie daje bowiem gwarancji, że osoba, która użyła klucza prywatnego jest tą, za którą się podaje. Gwarancję taką daje dopiero system certyfikacji kluczy.



Rys. 2. Konstrukcja przesyłki podpisanej elektronicznie przez nadawcę
Fig. 2. Structure of the document electronically signed by the sender

Certyfikat cyfrowy to elektroniczne zaświadczenie, że dane służące do weryfikacji podpisu elektronicznego są przyporządkowane określonej osobie i potwierdzają jej tożsamość. Certyfikacji dokonuje odpowiedni organ, poświadczający autentyczność danego klucza publicznego. Jest to tzw. Zaufana Trzecia Strona (*Trusted Third Party*). Zadaniem urzędu certyfikacji jest wydawanie i zarządzanie certyfikatami. Certyfikat zawiera następujące informacje: unikalny numer seryjny, tożsamość urzędu certyfikacji wydającego certyfikat, okres ważności certyfikatu, identyfikator właściciela certyfikatu (imię, nazwisko, pseudonim, e-mail itp.), klucz publiczny właściciela certyfikatu i podpis cyfrowy urzędu certyfikacji potwierdzający autentyczność certyfikatu. Maksymalna ważność certyfikatu kwalifikowanego wynosi 2 lata. Możliwe jest także unieważnienie lub zawieszenie certyfikatu, np. w przypadku poznania przez osoby niepowołane kodu PIN. Fakt ten zostaje odnotowany i opublikowany na tzw. liście CRL (*certificate revocation list*). Listę taką publikuje i uaktualnia codziennie na swoich stronach każdy kwalifikowany urząd certyfikacji.

Na polskim rynku działa kilka firm oferujących zestawy do składania bezpiecznego podpisu elektronicznego. Są to Krajowa Izba Rozliczeniowa (Szafir), Polska Wytwórnia Papierów Wartościowych (Sigillum), Unizeto Technologies (CERTUM), Enigma SOI (PEM-HEART) i EuroCert. W skład typowego zestawu wchodzą: czytnik kart kryptograficznych, karta kryptograficzna oraz zapisany na karcie certyfikat, który zawiera parę kluczy RSA, a także informacje o osobie na którą jest wystawiony. Ponieważ bezpieczny podpis elektroniczny weryfikowany jest tzw. certyfikatem kwalifikowanym, ma moc prawną odpowiadającą podpisowi odręcznemu i przy jego wystawianiu i wydawaniu weryfikowana jest tożsamość osoby.

Praktyka podpisu elektronicznego. Gorzej niż w teorii

Ministerstwo Gospodarki wymienia na swojej stronie internetowej następujące najważniejsze przypadki wykorzystywania certyfikowanego podpisu elektronicznego:

- kontakty drogą elektroniczną z Zakładem Ubezpieczeń Społecznych
- podpisywanie i składanie wniosków do Krajowego Rejestru Sądowego
- podpisywanie i wysyłanie raportów do Generalnego Inspektora Informacji Finansowej
- prowadzenie korespondencji z Generalnym Inspektorem Ochrony Danych Osobowych
- podpisywanie i wysyłanie deklaracji podatkowych do urzędów skarbowych
- podpisywanie faktur elektronicznych
- wymiana informacji z urzędami administracji publicznej
- składanie dyspozycji, przelewów, zmian w bankowości elektronicznej
- elektroniczne podpisywanie dokumentów w obrocie prawnym i handlowym
- podpisywanie wielu dokumentów elektronicznych jednocześnie
- podpisywanie ofert z wykorzystaniem certyfikatów kwalifikowanych na aukcjach i przetargach internetowych
- zawieranie umów przez Internet
- prowadzenie bezpiecznych transakcji elektronicznych przez Internet
- elektroniczne podpisywanie oświadczeń woli oraz dokumentów w obrocie prawnym

Powyższa lista jest jednak bardziej promocją niż informacją i dotyczy głównie podmiotów gospodarczych a nie osób prywatnych. Przykładem niech będą systemy uwiarygodniania w obsłudze bankowych kont internetowych – powszechnie stosowane tokeny, piny i zatwierdzania transakcji oraz poleceń kodem przesyłanym SMS-em. Ciekawym przykładem jest też używane coraz powszechniej oprogramowanie do internetowego składania rocznych deklaracji podatkowych PIT, w którym stosowane jest co prawda instrumentarium kryptografii asymetrycznej, ale rolę klucza prywatnego pełni kwota przychodów z wcześniejszej deklaracji. Podpis elektroniczny miał być narzędziem dla wszystkich, a mimo upływu już 14 lat, jest w zasadzie produktem niszowym, wykorzystywanym jedynie przez niektóre firmy i to w ograniczonym zakresie. Co więcej, zakres stosowania podpisu elektronicznego wyraźnie maleje. Statystyka aktywnych certyfikatów kwalifikowanych zgodnie ze stanem na dzień 6 maja 2014 według danych MG jest następująca [7]:

Liczba aktywnych certyfikatów kwalifikowanych: 295 158

Liczba certyfikatów wydanych od początku działalności podmiotów: 1 008 125

Natomiast liczba aktywnych firm w Polsce to ok. 1,8 mln (zarejestrowanych ok. 4 mln, 2013). Liczba dorosłych obywateli sięga liczby 27 mln (2010). Tylko 1% potencjalnych użytkowników dysponuje więc aktywnym podpisem kwalifikowanym. Natomiast aktywnych kart SIM mamy w kraju ponad 47 mln (2010), a przecież cyfrowa telefonia mobilna czyli telefonia komórkowa drugiej generacji (Era i Plus, 1996), jest równolatką technologii certyfikowanego podpisu elektronicznego (Certum, 1998). I co wydaje się zaskakujące, już teraz telefon komórkowy jest znacznie szerzej używany do różnych procedur weryfikacji i uwierzytelnienia niż podpis elektroniczny.

Skąd te problemy z podpisem?

Przyczyn jest tak wiele, ze trudno byłoby je wszystkie wymienić na kilku tylko stronach. Mają różnorodne źródła: użytkowe, prawne, techniczne, ekonomiczne, socjologiczne i jeszcze wiele innych. Do głównych wad podpisu elektronicznego należy przede wszystkim konieczność stosowania sprzętu i infrastruktury informatycznej (komputer, dostęp do Internetu) oraz płatnego zestawu do podpisu (czytnik do karty, karta kryptograficzna, certyfikat, program obsługi). Zgubienie lub kradzież klucza prywatnego grozi dramatycznymi konsekwencjami. Należy przy tym zauważyć, że samo używanie klucza prywatnego nakłada np. na osobę decyzyjną w firmie (90% aktywnych certyfikatów utrzymują firmy) szereg czynności, których osoba ta nie musiałaby osobiście wykonywać w przypadku podpisu odręcznego. Oto porównanie pracochłonności podpisu tradycyjnego i elektronicznego, na przykładzie podpisywania formularza KRS [5]:

- **Podpis własnoręczny, 4 czynności:** przygotowanie i wydruk wniosków, dołączenie załączników, podpisanie wniosku i przekazanie do wysłania.
- **Podpis elektroniczny, 7 czynności:** przygotowanie wniosków w formie elektronicznej, zeskanowanie załączników, podpisanie każdego z wniosków i załączników podpisem elektronicznym, załogowanie się na stronę systemu informatycznego, gdzie wysyłamy dokumenty, wybranie odpowiednich opcji i założenie nowej sprawy, wskazanie na swoim komputerze przygotowanych plików, wgranie ich do systemu i, po otrzymaniu informacji o wydaniu postanowienia, załogowanie się, i zachowanie postanowienia z podpisem elektronicznym na swoim komputerze.

Stosowanie podpisu elektronicznego może więc, zamiast oszczędzić pracy, wydatnie jej przysporzyć. Byłoby oczywiście łatwiej, gdyby kartę z czytnikiem oraz hasła i inne dane do logowania powierzono któremuś z pracowników (to jest nagminne w firmach). To jednak w gruncie rzeczy przekreśla sens stosowania podpisu elektronicznego, ale jak dotąd, nikomu to nie przeszkadza.

Nie mniej istotne są przyczyny natury prawnej. Środowisko prawne podpisu elektronicznego jest przestarzałe i nieprecyzyjne. Zarówno na w wymiarze unijnym jak i krajowym. Jednocześnie krytycznie zawęża się liczba zastosowań, w których podpis elektroniczny zwykły lub certyfikowany jest niezbędny by zastąpić podpis odręczny. Na przykład przy podpisywaniu umów. W zdecydowanej większości przypadków przepisy prawa nie wymagają, aby czynności prawne dokonywane były w formie pisemnej pod rygorem nieważności. Co do zasady zachowanie formy pisemnej jest konieczne tylko wtedy, gdy wynika to z konkretnego przepisu, a na dodatek w wielu przypadkach niezachowanie formy pisemnej nie skutkuje wprost nieważnością umowy. Forma pisemna zawsze będzie potrzebna np. w razie zawarcia umowy leasingu lub umowy przenoszącej autorskie prawa majątkowe lub umowy licencji wyłącznej. W innych przypadkach umowa może być zawarta w dowolnej formie.

Zatem w większości sytuacji życia codziennego i gospodarczego nie jest konieczne zawieranie umów w formie pisemnej pod rygorem nieważności, a to oznacza, że nie jest także konieczne – w razie zawierania takich umów w formie elektronicznej, stosowanie certyfikowanego podpisu elektronicznego. W praktyce składania podań i pism zwycięża system **ePUAP** i jego **profil zaufany**, czyli bezpłatna metoda potwierdzania tożsamości obywatela Polski w kontaktach z administracją, a także wspomniany już program **e-Deklaracje** Ministerstwa Finansów, który umożliwia składanie deklaracji podatkowych bez konieczności użycia kwalifikowanego podpisu elektronicznego.

Także i faktury elektroniczne mogą funkcjonować bez kwalifikowanego podpisu elektronicznego. Od początku można było korzystać równolegle z systemu **EDI**, a od stycznia 2013 r. także z innego dowolnego systemu. W bankowości natomiast stosowane są powszechnie własne metody poszczególnych banków (hasła, piny, tokeny i SMSy).

Dlatego też wydaje się, że już obecnie zdecydowaną większość użytkowników kwalifikowanego podpis elektronicznego stanowią po prostu klienci ZUS – użytkownicy programu Płatnik, którzy muszą mieć podpis kwalifikowany do przesyłania dokumentów rozliczeniowych ze względu na wyraźny zapis art. 47a § 2a ustawy o systemie ubezpieczeń społecznych. Jeśli ten przepis ulegnie zmianie (a jest to prawdopodobne, bo powstaje szereg nowych projektów dotyczących informatyzacji ubezpieczeń społecznych i służby zdrowia), podpis elektroniczny powołany Ustawą z 2001 r. i kolejnymi aktami prawnymi stanie się praktycznie zbędny.

Co dalej – biometria, podpis z mediatorem, kryptografia dynamiczna?

W kraju (m. in. w Instytucie Maszyn Matematycznych, wspólnie z firmami Hitachi oraz Mobile Experts) prowadzi się prace nad rozwojem biometrycznego podpisu elektronicznego, przeznaczonego przede wszystkim dla administracji publicznej. W dobie coraz powszechniejszego wykorzystania biometrii np. w systemach bankowych zastosowanie tej technologii wydaje się być interesującym rozwiązaniem. Głównym założeniem projektu jest uwolnienie użytkownika od posiadania karty kryptograficznej i stworzenie infrastruktury pozwalającej na złożenie podpisu elektronicznego w dowolnym miejscu. Konieczne byłoby wtedy przechowywanie kluczy prywatnych jak i wzorców biometrycznych każdego użytkownika w zabezpieczonej bazie danych Przy pomocy jednej z technologii biometrycznych, np. odczytu wzoru naczyń krwionośnych palca, każda osoba zarejestrowana w systemie mogłaby się uwierzytelnić. Technologicznie taki podpis nie różnił by się niczym od tradycyjnego podpisu elektronicznego złożonego przy użyciu karty kryptograficznej.

Wątpliwości budzi jednak bezpieczeństwo cech biometrycznych oraz kluczy prywatnych w bazie danych systemu, które byłoby zależne od sposobu zabezpieczeń oraz uczciwości instytucji dane te przechowującej. Problemem jest także wysoka cena zaufanych czytników biometrycznych. Technologia ta prawdopodobnie nie przyjęłaby się w domowych zastosowaniach. Terminale pozwalające na skorzystanie z systemu musiałyby być instalowane w miejscach użyteczności publicznej. Co więcej, podpis biometryczny nie zapewnia użytkownikowi wyłącznej kontroli nad danymi oraz urządzeniem do składania podpisów, a więc w myśl obowiązujących teraz przepisów, nie może być podpisem kwalifikowanym.

Drugą rozwijającą się prężnie technologią jest tak zwany podpis z mediatorem. Jest to stosunkowo nowe krajowe rozwiązanie, które polega na stworzeniu trzeciej strony biorącej aktywny udział w procesie składania podpisu elektronicznego., zwanej *finalizatorem*. Jest to technicznie możliwe dzięki podzieleniu klucza prywatnego na dwie części. Jedna zapisana jest na karcie kryptograficznej, na której generowany jest *prepodpis*. Dopiero

finalizator przy użyciu prepodpisu oraz swojej części klucza prywatnego użytkownika jest w stanie wygenerować właściwy podpis elektroniczny. Zaletą tego rozwiązania jest możliwość sprawdzenia ważności certyfikatu przez trzecią stronę. Jeśli certyfikat jest nieważny to nie dojdzie do finalizacji. Podpis z mediatorem nie zapewnia jednak interoperacyjności z innymi projektami eID ani z podpisem elektronicznym implementowanym w krajach Unii Europejskiej, ponieważ nie ma żadnych norm europejskich opisujących choćby proces generowania podzielonego klucza prywatnego innych istotnych elementów systemu.

Kryptografia dynamiczna

Inna procedura podpisu elektronicznego może być teoretycznie zrealizowana za pomocą algorytmów *kryptografii dynamicznej* [9, 10], które nie wymagają istnienia klucza publicznego w jawnej postaci. Kluczem jest sam szyfrogram. Wyeliminowanie wymiany kluczy kryptograficznych pomiędzy nadawcą a odbiorca wiadomości jest możliwe dzięki zastosowaniu tablic kryptograficznych, wygenerowanych wraz z szyfrogramem po stronie odbiorcy. Można wygenerować aż pięć rożnych rodzajów szyfrów, dzięki czemu informację sterującą można zaszyfrować innym szyfrem niż treść przekazywanej wiadomości. W takim szyfrogramie informacje sterujące, a więc klucze nie musza być już szczególnie utajnione. Klucze służące do deszyfracji są generowane w sposób dynamiczny po stronie odbiorcy wraz z odebranym szyfrogramem i jest zależny od czasu przetwarzania szyfrogramu. Otrzymujemy w ten sposób pierwszą właściwość systemu, a mianowicie niezależność od człowieka, który do tej pory był odpowiedzialny za bezpieczeństwo klucza prywatnego. Systemy oparte infrastrukturze klucza publicznego wymagają ponadto istnienia skomplikowanej zhierarchizowanej struktury związanej z zaufaną trzecią stroną oraz rozbudowanego systemu drzew katalogowych LDAP: i nazw DN centrów certyfikacji.

W systemie kryptografii dynamicznej istnieją jedynie dwa elementy: *Standard* oraz Suplement. Standard to elementy stałe: model szyfru, model deszyfracji i tablice kryptograficzne. Suplement to elementy zmienne: generatory permutacji, zmienna TIME i sposób jej wygenerowania, zasada utworzenia tablic kryptograficznych, zasada szyfrowania i deszyfracji strumieni danych. Na bezpieczeństwo systemu bardzo ważny wpływ ma fakt, że klucz kryptograficzny zmienia się w ciągu milisekund i jest ściśle zintegrowany z systemem. Nie ma więc zagrożeń związanych z zarządzaniem kluczami kryptograficznymi.

Bardzo ważną cechą systemu kryptografii dynamicznej jest automatyzm. Cały proces przekazywania, szyfrowania i podpisywania odbywa się bez udziału człowieka. Pozwala to na seryjne zastosowanie szyfrów w wielu obszarach życia gospodarczego. Automatyzm pozwala na szyfrowanie transmisji danych w systemach komunikacji głosowej, mapach z systemów geosatelitarnych, wreszcie na systemach architektury klient-serwer, które generują automatyczne raporty. Mogą być on zastosowane na przykład w elektronicznym głosowaniu do generowania automatycznych raportów z przebiegu głosowania i bezpiecznego przekazywania wyników z poszczególnych okręgów wyborczych. Również w bankowości automatyczne raporty generowane w poszczególnych oddziałach na koniec dnia będą mogły być bezpiecznie przekazywane do centrali banku. Możliwości szyfrowania i podpisywania korespondencji seryjnej są nieocenione. Bez konieczności osobnego podpisywania każdej wiadomości będzie możliwe na przykład wysyłanie decyzji zarządu spółki do jej wszystkich członków. Na bazie kryptografii dynamicznej stało się możliwe uproszczenie wielu usług PKI, na przykład usług notarialnych potwierdzających prawidłowość i ważność podpisu elektronicznego, potwierdzenie złożenia danych, weryfikacja kompletności wniosków itp. Dobrze odwzorowane są usługi niezaprzeczalności: identyfikacja nadawcy i odbiorcy jest realizowana poprzez szyfrowanie nagłówka, w którym zawarte są dane identyfikujące, tj. adres, czas nadania itd. Zastosowanie trzech rodzajów tablic kryptograficznych oraz zmiany szyfru w zależności od czasu i zasad szyfrowania, umożliwiło przesyłanie wiadomości w sieciach komputerowych i ich identyfikacje w każdym węźle automatycznie.

Nie wiadomo jeszcze jednak, czy kryptografia dynamiczna, rozwijana w naukowych ośrodkach wrocławskich od lat 90. ubiegłego wieku w ogóle będzie mogła być skutecznie wykorzystana do uwierzytelniania transmisji informacji cyfrowych. Istnieją niezależne opracowania, które wskazują na niekonsekwencje twórców kryptografii dynamicznej [11]. Stwierdzono np. że zaproponowana metoda nie jest „kryptograficznym perpetuum mobile", a niezauważonym przez autora metody kluczem jest informacja niezbędna do wygenerowania tablicy kryptograficznej przeznaczonej do zaszyfrowania „informacji sterującej" służącej wraz ze wspomnianą tablicą kryptograficzną do wygenerowania jednorazowego klucza sesyjnego dla prostego algorytmu podstawieniowego. Sposób przedstawienia metody nie daje ponadto możliwości: zaimplementowania podstawowych algorytmów oraz ocenienia efektywności procesu szyfrowania i deszyfrowania.

Nowe aplikacje górą

Wygląda na to, że nieruchawy i umierający moloch prawno-biurokratyczny, powołany do życia, powtórzmy, *Ustawą z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450)* oraz *Rozporządzeniem Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094),* a także kilkudziesięcioma następnymi aktami prawnym już uległ zamrożeniu. Licznik zdeterminowanych klientów podpisu elektronicznego zatrzymał się na poziomie 300 000. Bo tak naprawdę nikomu nie udało się jeszcze zrobić uniwersalnego narzędzia do wszystkiego. Wyspecjalizowani harcownicy przejmują ten rynek usług. Inne, prostsze aplikacje jak np. *ePUAP* i jego *profil zaufany*, *e-Deklaracje* Ministerstwa Finansów, *EDI (Electronic Data Interchange)*, smartfony, tablety, a w nich hasła, piny, tokeny i SMS-y wyraźnie zdobywają rynek. Jak na razie podpis elektroniczny utrzymuje głównie Zakład Ubezpieczeń Społecznych.

Literatura

[1] portal.etsi.org/esi/documents/e-sign-directive.pdf
[2] Daniel Wachnik: Rozporządzenie eIDAS – na pograniczu technologii i prawa, Elektronika – konstrukcje, technologie, zastosowania, nr 2/2014, str. 42-44.
[3] Dz.U. 2001 nr 130 poz. 1450.
[4] Dz.U. 2002 Nr 128 poz. 1094.
[5] http://prawo.money.pl/aktualnosci/okiem-eksperta/artykul/elektroniczna;rejestracja;spolki;z;o;o;nie;dziala;poprawnie,117,0,1156469.html
[6] R. L. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public-key cryptosystems, Magazine Communications of the ACM, Vol. 21 Issue 2, Feb. 1978, D.O.I. 10.1145/359340.359342.
[7] http://www.mg.gov.pl/Wspieranie+przedsiebiorczosci/Dzialalnosc+gospodarcza+i+e-przedsiebiorczosc/Podpis+elektroniczny
[8] http://ipwsieci.pl/wpis,64,Kilka_slow_o_bezpiecznym_podpisie_elektronicznym_weryfikowanym_kwalifikowanym_certyfikatem_wydanym_przez_kwalifikowany_podmiot_swiadczacy_uslugi_certyfikacyjne_.html.
[9] Mariusz Drożdż: Nowa jakość w ochronie informacji, czyli usługi w systemach kryptografii dynamicznej. Kwartalnik Prawo Mediów Elektronicznych, Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej (CBKE) Uniwersytetu Wrocławskiego, nr 4/2011.
[10] Zygmunt Topolewski: Komputerowe zabezpieczenie poufności informacji. Historia 40 lat wzlotów i upadków w badaniach naukowych. Wyższa Szkoła Handlowa, Wrocław 2008. ISBN 978-83-925470-4-4
[11] Ryszard Sobczak: Analiza metody szyfrowania ZT-Unitakod. Zeszyty Naukowe Wydziału ETI Politechniki Gdańskiej. Nr 4, seria: Technologie Informacyjne, 2006.